UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,868	02/28/2001	Michel Hazard	T2146-906833	3510

181 7590 12/09/2005

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 12/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/763,868	HAZARD, MICHEL	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/13/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's Request for Continued Examination filed on October 13, 2005. Claims 20-37 have been amended. Claims 20-38 are pending.

Response to Arguments

2. In response to applicant's argument in respect to independent claims 20 and 29 that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *an integrity check element is implemented from one end of the bus to the other with wiring diagram and its bus integrity controller; means for checking the integrity comprises parity generators and it is also specified that the parity generator calculates the parity of the data selected in the ROM; interrupting a normal operation of the microprocessor during the reading of an instruction whose code is "OO" or "FF"*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to Applicant's remark on pages 6-7 to the amended claims, the cited prior art, Holtey teaches that "the output of the access control (43) is applied as an enabling input to output buffer (52) during each memory read cycle. As a consequence, the transfer of information on the data bus is not secured when the output buffer is enabled...In Holtey the information is read in a memory block by a processor which is external to the chip".

However, the claimed language does not recite that the processors accessing and verify the sensitive information are the same processor that resides inside the chip. Examiner notes that the claim language of the steps of reading and verifying by "the processing means" do not distinguish itself to be equated to "said processing means" in the preamble which Examiner interprets to be a different processor that performs the verification of the sensitive information. Furthermore, even thought Applicant recites in the preamble that the transmitting of information through said data bus is secured but the body of the claim does not recite the steps of how to secure the data transmission through the data bus. In light of this interpretation, the cited prior art met the claim language of the independent claims as amended.

Applicant's arguments in respect to the amended claims 26, 33 and 34 (see remark pages 8 and 9) have been fully considered and are persuasive. Therefore, the rejection for claims 26-28 and 33-37 have been withdrawn. However, upon further consideration and in light of a newly found art, a new ground(s) of rejection is made for claims 20-38.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 20-23, 29-32 and 38 are rejected under 35 U.S.C. 102(b) as being anticipated by Holtey (U.S. Patent No. 5,442,704).

In respect to claim 20, Holtey discloses a method for protecting the processing of sensitive information in a security module having a monolithic structure, information processing means and storage means for storing information capable of being processed by said processing means, means for checking the integrity of information and at least a data bus, wherein the transmitting of information through said data bus is secure and in that it comprises the following steps (see Abstract):

selecting a piece of sensitive information stored in the storage means; determining a specific condition for the integrity of said information; reading, by the processing means, of said information transmitted from the storage means to the processing means for processing via a data bus (see Fig. 1, col. 3, line 15 - col. 4, line 29 and col. 5, line 39-col. 6, line 35);

processing the information and verifying by the processing means during processing that the specific condition is satisfied; and disabling processing of the information if the specific condition is not satisfied (see col. 4, lines 30-49, blocking access control met the limitation of disabling processing of the information).

In respect to claim 21, Holtey discloses the method according to claim 20, wherein the information is an operation code read in the storage means, all of the types of said operation code being contained in a table having a content determined during

the manufacture of the security module, and the specific condition for the integrity of the information being the value of said information is equal to one of several set values of the table (see col. 3, line 15 - col. 4, line 29).

In respect to claim 22, Holtey discloses the method according to claim 21, wherein said operation code to be processed is coded in the form of data bits and said bits do not all have the same binary value (see col. 3, lines 59-68).

In respect to claim 23, Holtey discloses the method according to claim 20, wherein the specific step of determining the condition for the integrity of said information comprises calculating a first piece of integrity data, by means for checking the integrity of information, using the information read in the storage means, comparing the first piece of integrity data to a second calculated piece of integrity data by means for checking the integrity of information, using the information received by said processing means and checking for equality, by said means for checking the integrity of information between the first and second pieces of integrity data (see col. 3, line 15-col. 4, line 49).

In respect to claim 29, the claim limitation is a system claim that is substantially similar to method claim 1. Therefore, claim 29 are rejected based on the similar rationale.

In respect to claim 30, Holtey discloses a security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table comprises at least a forbidden instruction value, the forbidden values being defined during the building of the module (see col. 3, lines 15-27).

In respect to claim 31, the claim limitation is a system claim that is substantially similar to method claim 23. Therefore, claim 31 is rejected based on the similar rationale.

In respect to claim 32, Holtey discloses the security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table, the security module comprising a means for reading an operation code and a disabling means activated during the reading of a forbidden operation code (see col. 3, lines 28-58).

In respect to claim 38, Holtey discloses the security module according to claim 29, characterized in that the security module is a microcircuit card (see col. 3, lines 15-27).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holtey (U.S. Patent No. 5,442,704) in view of Hog g et al. (U.S- Patent No. 4,281,216).

In respect to claims 24-25, Holtey discloses the method according to claim 23. Holtey does not disclose but Hogg discloses a piece of integrity data is calculated from at least one piece of calculation data whose value varies as a function of time or varies randomly (Hogg, Col. 9, lines 19-48). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the function of time with a pseudorandom number generator to varies a value taught by Hogg with Holtey's teaching of secure memory card with programmed controlled of security access for the benefit that there is no human knowledge of the generated keys (Hogg, Col. 19-32).

Claims 20-23, 26, 27, 29-34, 37 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al. (U.S. Patent No. 5,465,349, hereinafter Geronimi) in view of Anderson et al. ("Low Cost Attacks on Tamper Resistant Devices", http://www.Bellcore.com", 1996) and further in view of Takahira (U.S. Patent No. 4,930,129).

In respect to claim 20, Geronimi discloses a method for protecting the processing of sensitive information in a security module having a monolithic structure, information

processing means and storage means for storing information capable of being processed by said processing means, means for checking the integrity of information and at least a data bus, wherein the transmitting of information through said data bus is secure (Geronimi, col. 2, line 16-col. 3, line 32). Geronimi further discloses "prompting a break in the functioning of the circuit when abnormal condition are detected" (met the limitation of disabling processing of information if the specific condition is not satisfied) (see col. 1, lines 30-31). .

Geronimi does not explicitly disclose steps of selecting a piece of sensitive information stored in the storage means; determining a specific condition for the integrity of said information; reading, by the processing means, of said information transmitted form the storage means to the processing means for processing via a data bus. However, Anderson discloses attack on ciphertexts in which one-bit errors have been induced by environment stress such as ionizing radiation or some other comparable insult (Anderson, page 2, Differential Fault Analysis). Takahira discloses IC card having internal error checking capability of the recorded data (Takahira, col. 3, lines 22-28). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Geronimi's monitoring of abnormal integrated circuit operating condition and causing selective microprocessor interrupts with Anderson's attack that inducing one-bit errors by environment stress and Takashira's teaching of error checking of IC card stored data to provide tamper resistance device from environment stress.

In respect to claim 21, Geronimi, Anderson and Takahira disclose the method according to claim 20, wherein the information is an operation code read in the storage means, all of the types of said operation code being contained in a table having a content determined during the manufacture of the security module, and the specific condition for the integrity of the information being the value of said information is equal to one of several set values of the table (see Geronimi, col. 2, lines 41-51).

In respect to claim 22, Geronimi, Anderson and Takahira disclose the method according to claim 21, wherein said operation code to be processed is coded in the form of data bits and said bits do not all have the same binary value (see Geronimi, col. 2, lines 41-47).

In respect to claim 23, Geronimi, Anderson and Takahira disclose the method according to claim 20, wherein the specific step of determining the condition for the integrity of said information comprises calculating a first piece of integrity data, by means for checking the integrity of information, using the information read in the storage means, comparing the first piece of integrity data to a second calculated piece of integrity data by means for checking the integrity of information, using the information received by said processing means and checking for equality, by said means for checking the integrity of information between the first and second pieces of integrity data (see Takahira, col. 5, lines 27-49).

In respect to claim 26, Geronimi, Anderson and Takahira disclose the method according to claim 20, wherein the disabling of the processing of the information is performed by a microprogrammed instruction (see Geronimi, col. 2, lines 41-47).

In respect to claim 27, Geronimi, Anderson and Takahira disclose the method according to claim 26, wherein the microprogrammed instruction performs the following steps:

writing a piece of disable data into a nonvolatile location of the storage means (32, 33); and disabling the processing of the information (see Geronimi, col. 1, lines 30-32).

In respect to claim 29, the claim limitation is a system claim that is substantially similar to method claim 1. Therefore, claim 29 are rejected based on the similar rationale.

In respect to claim 30, Geronimi, Anderson and Takahira disclose a security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table, characterized in that the table comprises a forbidden instruction value (see Geronimi, col. 2, lines 41-47).

In respect to claim 31, the claim limitation is a system claim that is substantially similar to method claim 23. Therefore, claim 31 is rejected based on the similar rationale.

In respect to claim 32, Geronimi, Anderson and Takahira disclose the security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table, the security module comprising means for reading an operation code and a disabling means activated during the reading of a forbidden operation code (see Geronimi, col. 1, lines 50-63).

In respect to claim 34, Geronimi, Anderson and Takahira disclose the security module according to claim 29, comprising parity generators cooperating with the storage means, parity generators cooperating with the processing means, and a comparator connected to each of the parity generators and capable of inducing an interrupt in the processing means (Anderson, page 7, 3.2).

In respect to claim 37, the claim limitation is a system claim that is substantially similar to method claim 26. Therefore, claim 37 is rejected based on the similar rationale.

In respect to claim 38, Holtey discloses the security module according to claim 29, characterized in that the security module is a microcircuit card (see col. 3, lines 15-27).

5. Claims 24, 25, 28, 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al. (U.S. Patent No. 5,465,349, hereinafter Geronimi) in view of Anderson et al. ("Low Cost Attacks on Tamper Resistant Devices", http://www.Bellcore.com", 1996) and Takahira (U.S. Patent No. 4,930,129) and further in view of Kommerling et al. ("Design Principles for Tamper-Resistant Smartcard Processors", USENIX Worship on Smartcard Technology, May 10-11, 1999, hereinafter Kommerling).

In respect to claims, 24 and 25, Geronimi, Anderson and Takahira disclose the method according to claim 23. Geronimi, Anderson and Takahira do not disclose but Kommerling discloses wherein a piece of integrity data is calculated from at least one piece of calculated data whose value varies as a function of time or whose value varies randomly (Kommerling, 3.1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the integrity checking of information stored in the storage of an integrated circuit taught by Geronimi, Anderson and Takahira with the calculated data varies as a function of time or varies randomly taught by Kommerling to prevent the type of attack that require the attacker to predict the time at which a certain instruction is executed.

In respect to claim 28, Geronimi, Anderson and Takahira disclose the method according to claim 27. Geronimi, Anderson and Takahira do not explicitly disclose but Kommerling discloses reading by the processing means a nonvolatile location of the storage means upon power up of said module and disabling the module if a value read at this location does not match (see Kommerling, 3.3, the processor is designed such that it will not run after a power up without proper internal reset). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Kommerling's processor designed that prompt the malfunctioning of the processor upon detection of attack and will not run after the power up with the teaching of Geronimi, Anderson and Takahira's tamper resistant protection of smartcard result from environmental stress to prevent the device from being further tampering.

In respect to claim 33, the claimed limitation is similar to claim 28. Therefore, claim 33 is rejected based on the similar rationale.

In respect to claims 35 and 36, the claimed limitations are similar to claim 24 and 25. Therefore, claim 35 and 36 are rejected based on the similar rationale.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

December 5, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100